APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/712,988	11/12/2003	Ljupco Kocarev	2110-85-3	7343

7590   08/12/2009
GRAYBEAL JACKSON HALEY LLP
Suite. 350
155-108th Avenue N.E.
Bellevue, WA 98004-5973

EXAMINER
NGO, CHUONG D

ART UNIT	PAPER NUMBER
2193	

MAIL DATE	DELIVERY MODE
08/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 February 2009</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1,2 and 5-27</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) <u>13 and 14</u> is/are allowed.

6)☒ Claim(s) <u>1,2,5-10 and 15-27</u> is/are rejected.

7)☒ Claim(s) <u>11 and 12</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claim 20 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the

written description requirement. The claim(s) contains subject matter which was not described

in the specification in such a way as to reasonably convey to one skilled in the relevant art that

the inventor(s), at the time the application was filed, had possession of the claimed invention.

        In particular, the recitation "generating the first pseudo-random value from a previously

chaos-based pseudo-random value generated before the first chaos-based pseudo-random value"

in claim 20 is not supported by the specification.

2.   Claims 1,2,5-10 and 15-25 are rejected under 35 U.S.C. 101 because the claimed

invention is directed to non-statutory subject matter.

        For a claimed process to be patent-eligible under § 101, the process must (1) be tied to a

particular machine or apparatus that impose meaningful limits on the claim's scope to impart

patent-eligibility, or (2) transform a particular article into a different state or thing. (See

Diamondv. Diehr, 450 U.S. 175, 184 (1981); *Parker* v. *Flook,* 437 U.S. 584, 588 n.9 (1978);

Gottschalk v. Benson, 409 U.S. *63,* 70 (1972); *Cochrane* v. *Deener,* 94 U.S. 780,787-88 (1876),

and in *Bilski*). However, it is clear from claims 1,2,5-10 and 15-25 that the claimed method

does not transform a subject matter such as an article or material to a different state or thing.

Further, a mere recitation of "a computer-implemented method", "storing said chaos-based

pseudo-random sequence (Xn) in a circuit", and "generating encrypted data on a computer-

readable medium" in the claims are not drawn to any particular machine or apparatus, and thus

fail to tie the claimed method to a particular machine or apparatus that imposes meaningful limits

on the claim's scope. Therefore, the method of claims 1,2,5-10 and 15-25 fails to meet the

machine-or transform test, and thus is directed to a nonstatutory process.

3.   Claims 15-27 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Smeets

(6,813,625).

        As per claims 15,16,18,19,21,26 and 27, Smeets discloses in figure 2 a generation of a

chaos-based pseudo-random sequence in an encryption application, including generating (201) a

first pseudo-random value with a chaotic map, generating (800) a fist chaos-based random value

as a function of the first random value within a finite interval values, the function (exclusive-or

function) having an inverse with a plurality of branches, storing the first chaos-based random

value in a circuit and encrypting data using the stored first chaos-based random value as claimed

(see figure 10, and col. 10, lines 35-60). It is noted that Butler does not discloses random

sequence and the random value are pseudo. However, Butler does teaches in col. 6, line 33-37, a

pseudo random generation by keeping the external inputs IN[X] to the MISR constant.

Therefore, to a person of ordinary skill in the art it would have been an obvious modification

keep the external inputs IN[X] to the MISR constant as a seed for generating pseudo-random

sequence and value as claimed.

4.   As per claims 15,16,18,19,21,26 and 27, Smeets discloses in figure 2 a generation of a

chaos-based pseudo-random sequence in an encryption application including defining a chaotic

map (201) for generating a pseudo-random sequence of integer numbers in a certain interval,

choosing a seed (the initial states) for the pseudo-random sequence of integer numbers, and

generating numbers of the pseudo-random sequence (Z), defining a function F(203) on the

interval whose inverse has a plurality of branches and calculating numbers of a chaos-based

pseudo-random sequence by applying the function to corresponding integer numbers of the of

the pseudo-random sequence, storing the first chaos-based random value in a circuit and

encrypting data using the stored first chaos-based random value as claimed as claimed (see col.9,

lines 39-60).

As per claims 17,24 and 25, Smeets in col. 6, lines 1-5, the function F being also

exclusive-or function (mod2 sum) as that of the present invention and thus the inverse of the

function has a number of branches equal to the largest bound of the interval.

As per claims 22 and 23 Smeets discloses col.5, , lines 45-67 the chaotic map a truncated

linear congruential generator.

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

6.   Claims 15-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Butler

(6,678,707).

As per claims 15,16,18,19,21,26 and 27, Butler discloses in figure 8 a generation of a

chaos-based random sequence in an encryption application, including generating (402-412) a

first random value with a chaotic map, generating (800) a fist chaos-based random value as a function of the first random value within a finite interval values, the function (exclusive-or function) having an inverse with a plurality of branches, storing the first chaos-based random value in a circuit and encrypting data using the stored first chaos-based random value as claimed (see figure 10, and col. 10, lines 35-60). It is noted that Butler does not discloses random sequence and the random value are pseudo. However, Butler does teaches in col. 6, line 33-37, a pseudo random generation by keeping the external inputs IN[X] to the MISR constant. Therefore, to a person of ordinary skill in the art it would have been an obvious modification keep the external inputs IN[X] to the MISR constant as a seed for generating pseudo-random sequence and value as claimed.

As per claims 17, 24 and 25, Butler disclose in col. 8, lines 18-20, the function being also exclusive-or function as that of the present invention and thus the inverse of the function has a number of branches equal to the largest bound of the interval.

As per claims 22 and 23, Butler discloses in figure 3 the chaotic map a truncated linear congruential generator.

7.   Claims 11 and 12 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8.   Claims 13 and 14 are allowed.

9.   Applicant's arguments filed on 08/12/2008 have been fully considered but they are not persuasive.

Regarding to the rejection of claim 20 is rejected under 35 U.S.C. 112, first paragraph, it is respectfully submitted that the paragraph [54] discloses that the generation a pseudo-random sequence of bits is easily repeated for generators of sequences of pseudo-random numbers. However, it has never disclosed a generation of a pseudo-random value based on a previously chaos-based pseudo-random value. Therefore it does provide support for "generating the first pseudo-random value from" as recited in the claim.

Regarding to the rejection under 35 U.S.C. 101, it is respectfully submitted , the method of claims 1,2,5-10 and 15-25, as explained in the rejection, is not tied to a particular machine or apparatus that impose meaningful limits on the claim's scope to impart patent-eligibility, or transform a particular article into a different state or thing, and thus fails to meet the machine-or transform test, and therefore, is directed to a nonstatutory process.

Regarding to the rejection of claims 15-27 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Smeets. It is respectfully submitted Smeets clearly disclose the random numbers generation based on pseudo random noise sequences (PN sequence), and thus clearly teaches a chaos-based pseudo-random value as claimed.

Applicant's arguments regarding to Butler have been considered but are moot in view of the new ground(s) of rejection.

10.   The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11.   Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Chuong D. Ngo whose telephone number is (571) 272-3731. The
examiner can normally be reached on Monday-Friday.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Lewis, Jr. A. Bullock can be reached on (571) 272-3759. The fax phone number for
the organization where this application or proceeding is assigned is 571-273-8300.

        Information regarding the status of an application may be obtained from the Patent
Application Information Retrieval (PAIR) system. Status information for published applications
may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
applications is available through Private PAIR only. For more information about the PAIR
system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR
system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would
like assistance from a USPTO Customer Service Representative or access to the automated
information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

                                                /Chuong D Ngo/
                                                Primary Examiner, Art Unit 2193
09/11/2009